

**Remarks:**

Claims 1-20 are pending in the current application and rejected under 35 U.S.C. § 102 and § 103. Claims 1, 11 and 13-17 have been amended. No new matter has been added. Support for the amendments is found within the claims, the specification, and the drawings. It is submitted that the application, as amended, is in condition for allowance.

**§ 102 Rejection(s):**

Claims 1-3, 5-7, and 11-20 are rejected as being anticipated by U.S. Patent No. 6,463,300 (Oshima). It is respectfully noted that anticipation of a claim under 35 U.S.C. §102 (a), (b) and (c) requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," that "[t]he identical invention must be shown in as complete detail as is contained in the ... claim" and "[t]he elements must be arranged as required by the claim." M.P.E.P. §2131.

The instant application is directed to transparently reconfiguring configuration data required to operate a mobile device on a communications network for a particular operator, where the configuration data is not stored in the SIM card. More particularly, Claim 1, as amended, recites a method of transparently configuring a mobile device in a mobile communications network with the mobile device's identity module respective configuration data comprising: determining whether a first identity module coupled to a mobile device is different from a second identity module previously coupled to the mobile device; searching entries in a data structure for first configuration data associated with the first identity module in response to determining the first identity module is different from the second identity module, wherein said data structure has a plurality of entries comprising configuration data for corresponding plurality of identity modules that can be coupled to said mobile device, wherein the configuration data comprises network access information allowing the mobile device to operate in the mobile communications network using the first identity module without need for externally programming the mobile device with the network access information; and configuring the mobile device to use the first configuration data, when said first configuration data is present in an entry of the data structure. Claims 11 and 17, as amended, are directed to a method and mobile device for transparently configuring a mobile device coupled to a new identity module with the new identity module respective configuration data and substantially incorporate the amendments of Claim 1.

Oshima is directed to a mobile communication device and method for determining whether or not a user of a device is permitted to use the device when the device's IC/SIM card has been replaced since the last access to a communication network (col 3, lines 38-42). The main object of Oshima's

disclosure is to prevent an unauthorized person from using a mobile communications device ( col. 3, lines 1-18). If the SIM card is not exchanged, the user is queried for a SIM-card specific (i.e. user-specific) PIN number before the device can access the network (col. 9 lines 53-58, col. 10 lines 31-48). Oshima discloses querying a user for a secret number stored in the mobile device when a SIM card is exchanged (col. 9 lines 53-63). If the secret number is inputted, the user is then queried for a PIN number (col. 9 line 53 – col. 10 line 3, col. 11 lines 12-26). If the PIN number is input, the SIM data storing section of the mobile device is updated and the device can connect to the network (col. 11 lines 30-33).

Oshima fails to disclose searching entries in a data structure for first configuration data associated with the first identity module in response to determining the first identity module is different from the second identity module, wherein said data structure has a plurality of entries comprising configuration data for corresponding plurality of identity modules that can be coupled to said mobile device, wherein the configuration data comprises network access information to allow the mobile device to operate in the mobile communication network using the first identity module without need for externally programming the mobile device with the network access information. On page 3 of the Office Action, the Examiner alleges that Oshima discloses searching entries in a data structure for first configuration data associated with the first identity model (col. 6 lines 28-48, col. 7 lines 25-35). The Applicant respectfully disagrees.

Oshima discloses querying a user for a secret number and a PIN number when the SIM card is exchanged (i.e. in response to determining the first identity module is different from the second identity module) (col. 9 line 53 – col. 10 line 3, col. 11 lines 12-26). If the secret number and PIN number are input successfully, Oshima discloses updating the SIM data storing section of the memory section of the mobile device and connecting to the network (col. 11 lines 27-33). Thus, Oshima fails to disclose searching entries in a data structure for first configuration data associated with the first identity module in response to determining the first identity module is different from the second identity module. Rather, Oshima discloses updating the mobile device memory with data directly from the SIM card in response to successive successful user inputs.

Further, Oshima fails to disclose a data structure with a plurality of entries comprising configuration data for corresponding plurality of identity modules that can be coupled to said mobile device. On pages 3-4 of the Office Action, the Examiner alleges that Oshima inherently suggests the mobile terminal couple store a plurality of IC cards data for subsequent data comparison. The Applicant respectfully disagrees with this observation, since according to Oshima's disclosure, the abovementioned data is used to "...recognize that the attached SIM card is exchanged..." (col. 9, lines 54-59). Applicant

respectfully requests Examiner point out the portions of the cited reference that suggest all such elements with specificity if the rejection is maintained.

Oshima discloses a table comprising at least one pair of an address number and a storing data which is stored a memory of the SIM card indicated in the address number (col. 7 lines 33-44). The stored data is not updated unless the SIM card is exchanged or the SIM card address number is updated (step S24), and only after the user successfully inputs a secret number or PIN (col. 8 lines 8-60, col. 11 lines 27-29). The stored data is updated with second data (personal data inputted by the user) and does not comprise configuration data for a corresponding identity module (col. 7 line 65 - col. 8 line 7). Oshima discloses using a plurality of a pair of the address number and stored data to reduce probability of accidental coincidence where the stored data coincides with the data in an exchanged SIM card (col. 8 lines 61-67). Thus, Oshima does not disclose a plurality of entries comprising configuration data for corresponding *plurality of identity modules*.

Oshima also fails to disclose a data structure for first configuration data associated with the first identity module, wherein the configuration data comprises network access information allowing the mobile device to operate in the mobile communication network using the first identity module without need for externally programming the mobile device with the network access information. On page 4 of the Office Action, Examiner alleges that Oshima discloses configuration data comprising network access information needed to allow the mobile device to operate in the mobile communications network without the need for externally programming the mobile device. The Applicant respectfully disagrees.

Configuration data comprises information related to processing, routing and timing of communication data, such as an access point name, a wireless access point internet protocol, a web gateway IP address, a short messaging service center, system identification code, and other system or environment dependent codes (Fornell [0009], [0043-0044]). Most service providers require a mobile device be configured with network access information for the particular provider. As noted in the application, not all necessary configuration data is stored in a identity module, and therefore if an exchanged identity module does not comply with the previously stored configuration data corresponding to an operator or service provider, the mobile device will not be able to access the desired network (see Fornell [0010-0011]). The instant disclosure is directed to transparently reconfiguring configuration data required to operate a mobile device on a communications network for a particular operator, where the configuration data is not stored in the identity module, but maintained independently from the identity module.

Oshima discloses a SIM card storing an IMSI number, a telephone number data of a subscriber, and a short dial data registered by a user (col. 7 lines 24-26). While Oshima may disclose storing some configuration data in the SIM card, Oshima fails to disclose a method for storing all the necessary network access information such that the mobile device can operate in the mobile communication network using a SIM card corresponding to another operator or service provider without the need for externally programming the mobile device with the network access information. Thus, Oshima requires at least some additional configuration data to be externally programmed in the mobile device if the exchanged SIM card corresponds to a new operator or service provider.

In view of the above arguments, it follows that Oshima also fails to disclose configuring the mobile device to use the first configuration data, when said first configuration data is present in an entry of the data structure. On page 3 of the Office Action, Examiner suggests that Oshima discloses configuring the mobile device to use the first configuration data, when the controller recognizes the SIM card is not exchanged and going through steps S11-S14 (col. 9 lines 54-59, col. 10 lines 31-46). The Applicant respectfully disagrees. Rather, Oshima discloses reading a PIN number from the SIM card, querying the user for inputting the PIN number, and if the input number is equal to the PIN number, the user is allowed to connect to the internet (col. 10 lines 31-46). The cited method of Oshima is directed to limiting access to the mobile device when the SIM card is unchanged. Oshima does not disclose, teach, or suggest configuring the mobile device to use the first configuration data, when said first configuration data is present in an entry of the data structure.

Oshima fails to disclose each and every element as set forth in Claim 1, as amended, in as complete detail as is contained in the claim or as required by the claim. Accordingly, it is respectfully requested that the rejection of Claim 1 under 35 U.S.C. § 102 be withdrawn. It is respectfully submitted Claims 2-3 and 5-7 depend on Claim 1 and should be in condition for allowance by the virtue of their dependence on an allowable base claim.

Claims 11 and 17, as amended, substantially incorporate the amendments of Claim 1. Therefore, for the same reasons as set forth above in regards to amended Claim 1, Claims 11 and 17 should be also in condition for allowance. It is respectfully submitted Claims 13-16 and 18-20 depend on Claims 11 and 17, respectively, and should be in condition for allowance by the virtue of their dependence on an allowable base claim. Accordingly, Applicant respectfully requests the rejection of Claims 11 and 13-20 under §102 in view of Oshima also be withdrawn.

**§ 103 Rejection(s):**

Claims 4 and 8-10 are rejected as being obvious under U.S. Patent No. 6,463,300 (Oshima) in view of US Publication 2004/0195313 (Lee).

Lee is directed to methods for updating newly received network information or additional network information (paragraph [0009]). The object of Lee is to solve the problem requiring network information to be set up multiple times when a smart card is transported to another mobile terminal when a user switches or purchase mobile terminals. Lee teaches receiving system network set-up information into a mobile terminal from a wireless communication system and connecting a smart card in the mobile terminal and determining if there exists network set-up information in the smart card (paragraph [0011]). If no network information is found in the smart card, the newly-acquired network set-up information is stored in a network set-up information file stored in the smart card. If there is existing network set-up information stored in the smart card, the newly-acquired network set-up information is compared to the existing network set-up information, and updating difference between the existing network set-up information and the newly-acquired system network set-up information in the network set-up information file if there is the network set-up information present in the smart card.

Applicant respectfully traverses the Examiner's rejection. MPEP §2143 provides "the prior art reference (or references when combined) must teach or suggest all the claim limitations." As discussed above, Oshima fails to disclose each and every element of Claims 1 and 17. Lee does not disclose, teach, or suggest (1) searching entries in a data structure for first configuration data associated with the first identity module in response to determining the first identity of module is different from the second identity model, wherein said data structure has a plurality of entries comprising configuration data for corresponding plurality of identity modules that can be coupled to said mobile device, wherein the configuration data comprises network access information to allow the mobile device to operate in the mobile communication network using the first identity module without need for externally programming the mobile device with the network access information; or (2) configuring the mobile device to use the first configuration data, when said first configuration data is present in an entry of the data structure.

Lee fails to disclose, teach, or suggest searching entries in a data structure for first configuration data associated with the first identity module in response to determining the first identity of module is different from the second identity model, wherein said data structure has a plurality of entries comprising configuration data for corresponding plurality of identity modules that can be coupled to said mobile device, wherein the configuration data comprises network access information to allow the mobile device to operate in the mobile communication network using the first identity module without need for

externally programming the mobile device with the network access information. Rather, Lee teaches receiving network setup information from the network (i.e. downloading network setup information from a network), whenever the device is used (paragraph [0023], FIG. 2, S200). The mobile terminal checks the smart card (i.e. identity module) for network setup information (S201, S202).

Lee teaches comparing the received information with information in the smart card (S203, S204), as opposed to searching a data structure for entries. Lee also fails to teach or suggest a data structure having a plurality of entries comprising configuration data for corresponding plurality of identity modules that can be coupled to said mobile device. The method in Lee only corresponds to the single identity module (i.e. smart card) currently coupled to the mobile device. Further, Lee fails to disclose and, in fact, teaches away from a method that allows the mobile device to operate in the mobile communication network using the first identity module without need for externally programming the mobile device with the network access information (“receiving network information from mobile network” S200, “directly entering network information into mobile terminal” S300).

Additionally, Lee fails to disclose configuring the mobile device to use the first configuration data, when said first configuration data is present in an entry of the data structure. Rather, Lee teaches that comparing the received information with the information on the smart card, and updating the network set-up information file according to the differences (paragraph [0025], S204). Lee does not disclose configuring the mobile device, but rather updating the network setup information stored in the smart card.

On pages 8-9 of the Office Action regarding Claim 4, Examiner states that Lee teaches storing a reference to the first identity module in a second entry, wherein the first entry is associated with the second entry, such that when the first identity module is recoupled to the mobile device after being removed, the reference in the second entry is used to access the first configuration data stored in the first entry. Applicant respectfully disagrees. Lee teaches receiving network setup information from the network (i.e. downloading network setup information from a network), whenever the device is used (paragraph [0023], FIG. 2, S200), checking the smart card (i.e. identity module) for network setup information (S201, S202), and then comparing the two sets of information (S203, S204). A reference in a second entry is not used to access stored configuration data, but rather Lee teaches reconnecting to the network to receive setup information each time an identity module is recoupled, and then proceeding through steps S201-S204.

Thus, even if the two references can be combined, Lee fails to cure the deficiencies of Oshima. Accordingly, Applicant respectfully requests the rejection of Claims 4 and 8-10 under § 103 be withdrawn.

**Conclusion:**

For the above reasons, neither Oshima nor Lee, alone or in combination, disclose, teach, or suggest the invention as recited in the claims. Therefore, it is respectfully submitted that Claim 1 is in condition for allowance. Claims 2-10 depend on Claim 1 and should be in condition for allowance by the virtue of their dependence on an allowable base claim. Claims 11 and 17 substantially incorporate the elements of Claim 1, therefore Claims 11 and 17, and Claims 13-16 and 18-10 depending from Claim 11 and 17 respectively, should also be in condition for allowance. Accordingly, it is respectfully requested that the rejection of the claims under 35 U.S.C. § 102 and § 103 be withdrawn.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein; and no amendment made was for the purpose of narrowing the scope of any claim, unless Applicants have expressly argued herein that such amendment was made to distinguish over a particular reference or combination of references.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles, California, telephone number (310) 789 2100 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

Date: January 30, 2008

By: /F. Jason Far-hadian /  
F. Jason Far-hadian, Esq.  
Registration No. 42,523

Customer No. 42698